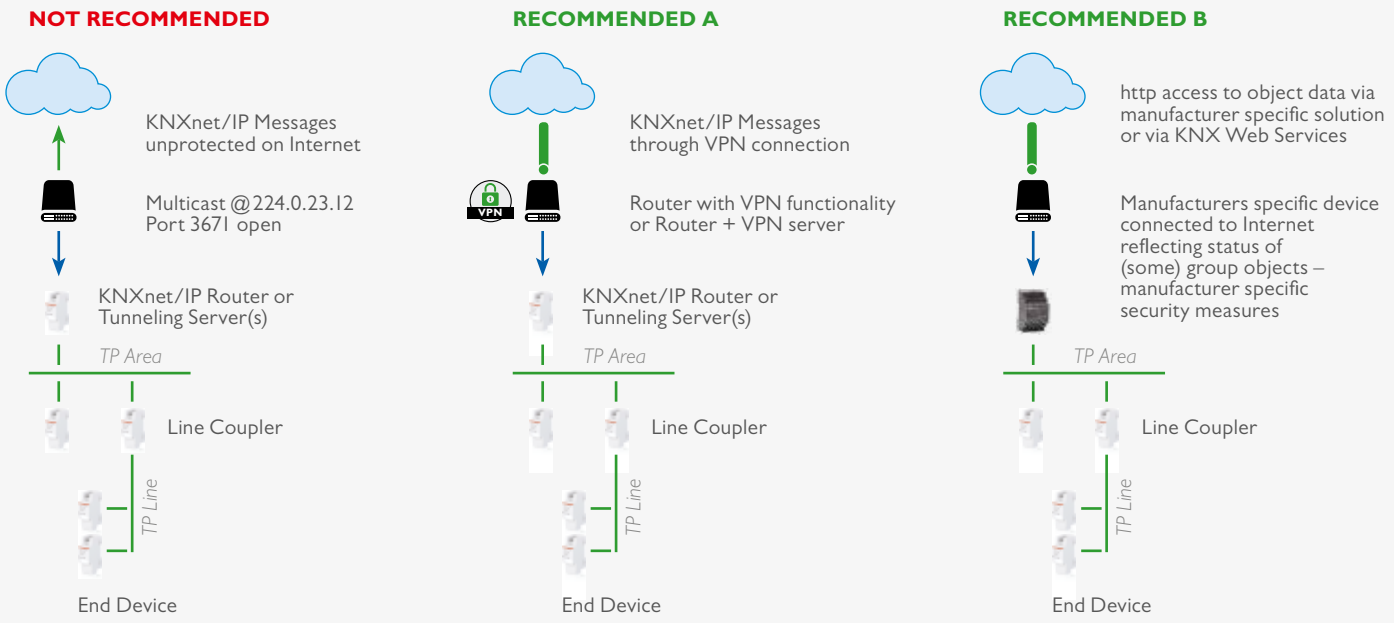
Smart home and building solutions.
Global. Secure. Connected.

KNX SECURE

KNX-STANDPUNTNOTA OVER
DATAVEILIGHEID EN PRIVACY

Dit document is bedoeld als een gids voor zowel installateurs als KNX-fabrikanten. Hierin komen ze meer te weten over de huidige maatregelen die ze kunnen ondernemen om de veiligheid van KNX-installaties te verhogen.

TOEGANG TOT HET NETWERK VOOR VERSCHILLENDE FYSIEKE KNX-MEDIA VOORKOMEN



Toegang tot KNX-netwerken via internet

Een goed beveiligingsconcept berust op een goede preventie tegen ongeoorloofde toegang. In geval van een KNX-installatie houdt dit in dat alleen bevoegde personen (de installateur, de beheerder, de gebruiker) fysieke toegang tot de KNX-installatie mogen hebben. Bij het ontwerp en de installatie moeten de kritieke elementen van elk KNX-medium op de best mogelijke manier worden beschermd.

Installatie van kabels en apparaten

- Over het algemeen worden toepassingen en apparaten goed bevestigd om te voorkomen dat ze gemakkelijk kunnen worden verwijderd, waardoor onbevoegden toegang tot een KNX-installatie zouden krijgen.
- Behuizingen en verdeelborden met KNX-apparaten moeten goed worden afgesloten of in ruimten worden geplaatst die enkel toegankelijk zijn voor bevoegde personen.
- Buiten worden apparaten op voldoende hoogte gemonteerd (bv. weerstation, windsensor, bewegingsdetector ...).
- In openbare ruimten die niet voldoende worden bewaakt, moet er worden overwogen om gebruik te maken van conventionele apparaten met binaire ingangen. Deze worden op beschermde plaatsen (bv. in verdeelborden) of drukknopinterfaces geplaatst zodat de toegang tot de bus wordt verhinderd.
- Indien beschikbaar moeten de antidiefstalmaatregelen, die bepaalde applicatiemodules aanbieden, worden gebruikt (bv. apparaten bevestigen met behulp van schroeven, die enkel met gereedschap kunnen worden verwijderd en voldoende bescherming bieden tegen lostrekken ...).

Twisted Pair

- De kabeluiteinden mogen niet zichtbaar zijn of buiten de muur, zowel in als buiten het gebouw, hangen.
- Een buskabel buiten vormt een groter risico. De fysieke toegang tot een KNX Twisted Pair kabel moet in dit geval nog moeilijker worden gemaakt dan in het huis/gebouw zelf.

- Voor extra bescherming kunnen apparaten die in zones met beperkt toezicht zijn geïnstalleerd (buiten, ondergrondse parkeergarage, toilet enz.), op een extra lijn worden aangesloten. Door activering van de filtertabel in lijnkoppelingen conform punt 2 kan er worden voorkomen dat een hacker toegang tot de volledige installatie krijgt.

Powerline

- Om de inkomende en uitgaande signalen te filteren, worden er elektronische filters gebruikt.

Frequentie

- Aangezien radiofrequentie een open medium is, kunnen er geen fysieke beschermingsmaatregelen worden genomen die de toegang verhinderen. Daarom moeten er andere maatregelen worden genomen. Deze worden in punten 2 tot en met 5 (en met name in punt 4) vermeld.

IP

- Gebouwenautomatisering moet via een eigen LAN en WLAN met eigen hardware (routers, schakelaars enz.) werken.
- Ongeacht het type KNX-installatie moeten in ieder geval de gebruikelijke beveiligingsmechanismen voor IP-netwerken in acht worden genomen. Deze omvatten omvatten (maar zijn niet beperkt tot):

MAC-filters

- Encryptie van draadloze netwerken in combinatie met sterke wachtwoorden (wijziging van het standaardwachtwoord - WPA2 of hoger) en bescherming ervan tegen onbevoegden.
- Wijziging van de standaard-SSID (SSID is de naam waaronder een draadloos toegangspunt zichtbaar is in het netwerk, meestal fabrikant en producttype). Standaard-SSID's kunnen wijzen op productspecifieke zwakke punten van de gebruikte toegangspunten en zijn zo bijzonder kwetsbaar voor hackers. Het toegangspunt kan bovendien zo worden ingesteld dat 'beaconing' (periodieke verzending van onder meer de SSID) wordt voorkomen.
- Voor KNX IP multicast moet er een ander IP-adres dan het standaardadres (224.0.23.12) worden gebruikt. Een geschikt adres kan met de netwerkbeheerder worden overeengekomen.
- Bij grotere projecten waarbij de aansluiting op KNXnet/IP is vereist, wordt er een beroep op IT-netwerkspecialisten gedaan. Op deze manier kan de netwerkconfiguratie nog worden geoptimaliseerd (beheerde schakelaars, virtuele LAN, toegangspunten met IEEE 802.X enz.) en kunnen er verdere beschermingsmechanismen zoals e-mailfiltering en antivirus worden geïmplementeerd.

Internet

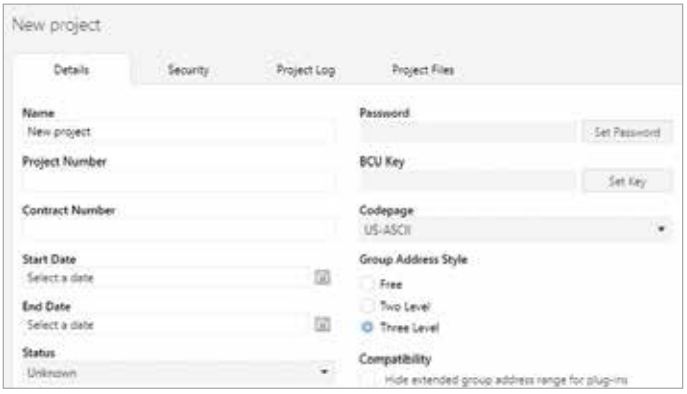
- KNXnet/IP-routing en KNXnet/IP-tunnelling zijn niet ontworpen voor gebruik via internet. Daarom raden we aan om geen poorten van routers naar internet te openen en zo KNX-communicatie via internet zichtbaar te maken.
  - De (W)LAN-installatie wordt door middel van een firewall beschermd.
  - IDe (W)LAN-installatie wordt door middel van een firewall beschermd.
  - Ingeval er geen externe toegang tot de installatie nodig is, kan de standaardgateway op 0 worden gezet. Op deze manier wordt elke communicatie met internet geblokkeerd.
- De toegang tot een installatie via internet is mogelijk op de volgende manier:
  - Toegang tot de KNX-installatie mogelijk maken via VPN-verbindingen: dit vereist echter een router die VPN-serverfunctionaliteit ondersteunt of een server met VPN-functionaliteit.
  - Alle fabrikantspecifieke oplossingen die op de markt beschikbaar zijn en visualisaties (bv. die http-toegang mogelijk maken).
  - KNX heeft in een uitbreiding op de KNX Standard een gestandaardiseerde KNX-oplossing gespecificeerd voor toegang tot KNX-installaties via webdiensten op internet.

ONGEWENSTE COMMUNICATIE BINNEN HET NETWERK BEPERKEN

- De individuele adressen van apparaten moeten correct overeenkomstig de topologie worden toegewezen en de routers moeten zodanig worden geconfigureerd dat ze geen berichten met een onjuist bronadres doorgeven. Op deze manier kan ongewenste communicatie tot één enkele lijn worden beperkt.
- Point-to-point en mogelijk broadcast communicatie tussen routers moet worden geblokkeerd. Op deze manier kan de herconfiguratie opnieuw tot één enkele lijn worden beperkt.
- De koppelaars moeten zodanig worden geconfigureerd dat ze de filtertabellen actief gebruiken en geen groepsadressen doorgeven die niet binnen een specifieke lijn worden gebruikt. Indien dit niet het geval is, bestaat het risico dat de communicatie in een specifieke lijn zich ongecontroleerd over de hele KNX-installatie verspreidt.

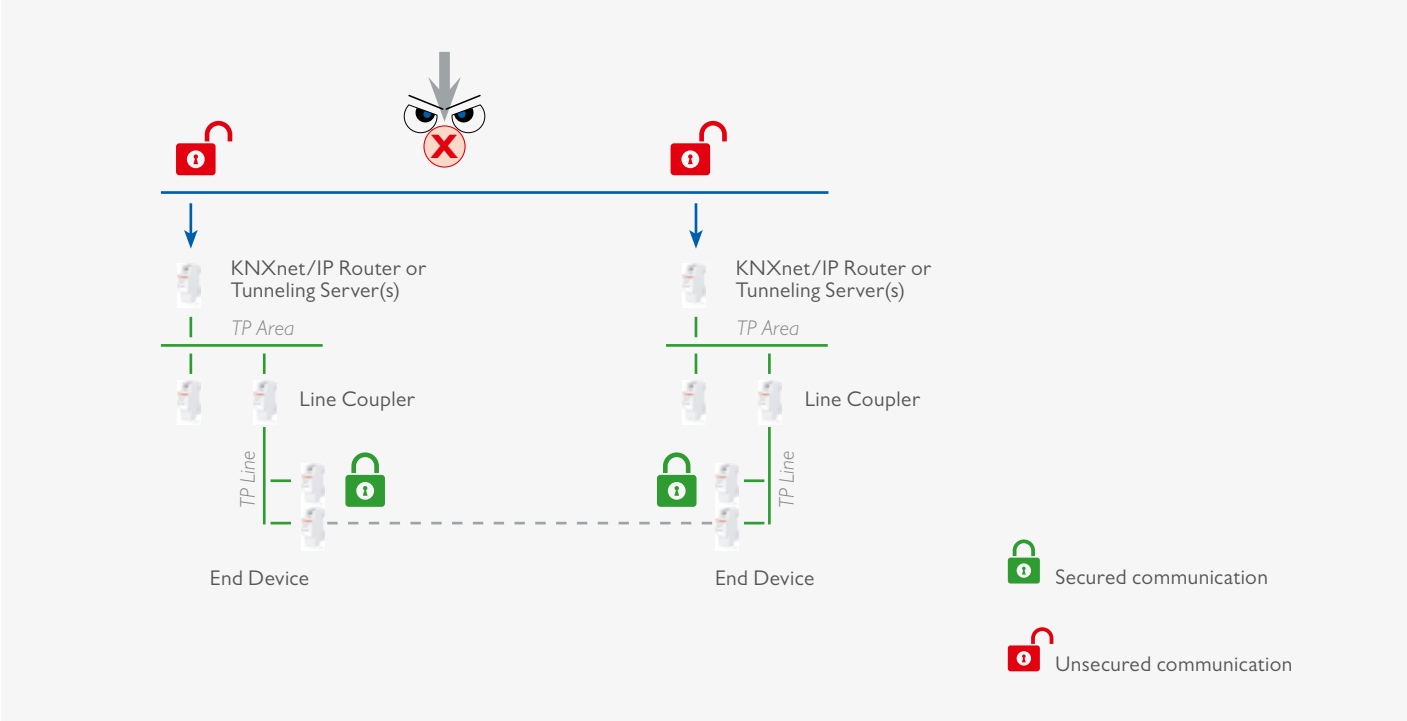
DE CONFIGURATIECOMMUNICATIE BESCHERMEN

ETS maakt het mogelijk om een projectspecifiek wachtwoord te definiëren waarmee apparaten tegen ongeoorloofde toegang kunnen worden vergrendeld. Zo voorkomt u dat onbevoegde personen de configuratie van de installatie kunnen lezen of wijzigen.



Configuratiecommunicatie in ETS beveiligen

DE RUNTIME COMMUNICATIE BESCHERMEN



KNX-runtime communicatie op een IP-netwerk met KNXnet IP Security beveiligen

- Naast de hierboven vermelde maatregelen kan de runtime communicatie van KNX worden beschermd via de gespecificeerde
  - KNX Data Secure en
  - KNX IP Secure mechanismen
- KNX Data Secure zorgt ervoor dat, ongeacht het gekozen KNX-medium, berichten die via KNX-apparaten worden verstuurd, kunnen worden geauthenticeerd en/of gecodeerd.

Om dit te verzekeren, zelfs ingeval dergelijke communicatie niet zou zijn beveiligd en dergelijke netwerken met IP zouden zijn verbonden, werden boven op dit alles de KNX IP Secure mechanismen gedefinieerd. Op deze manier wordt er verzekerd dat KNX IP-tunnelling- of routingberichten niet kunnen worden opgenomen of gemanipuleerd op IP. De KNX IP Secure mechanismen zorgen ervoor dat het volledige KNXnet/IP-dataverkeer in een 'veiligheidsdeken' wordt gewikkeld.

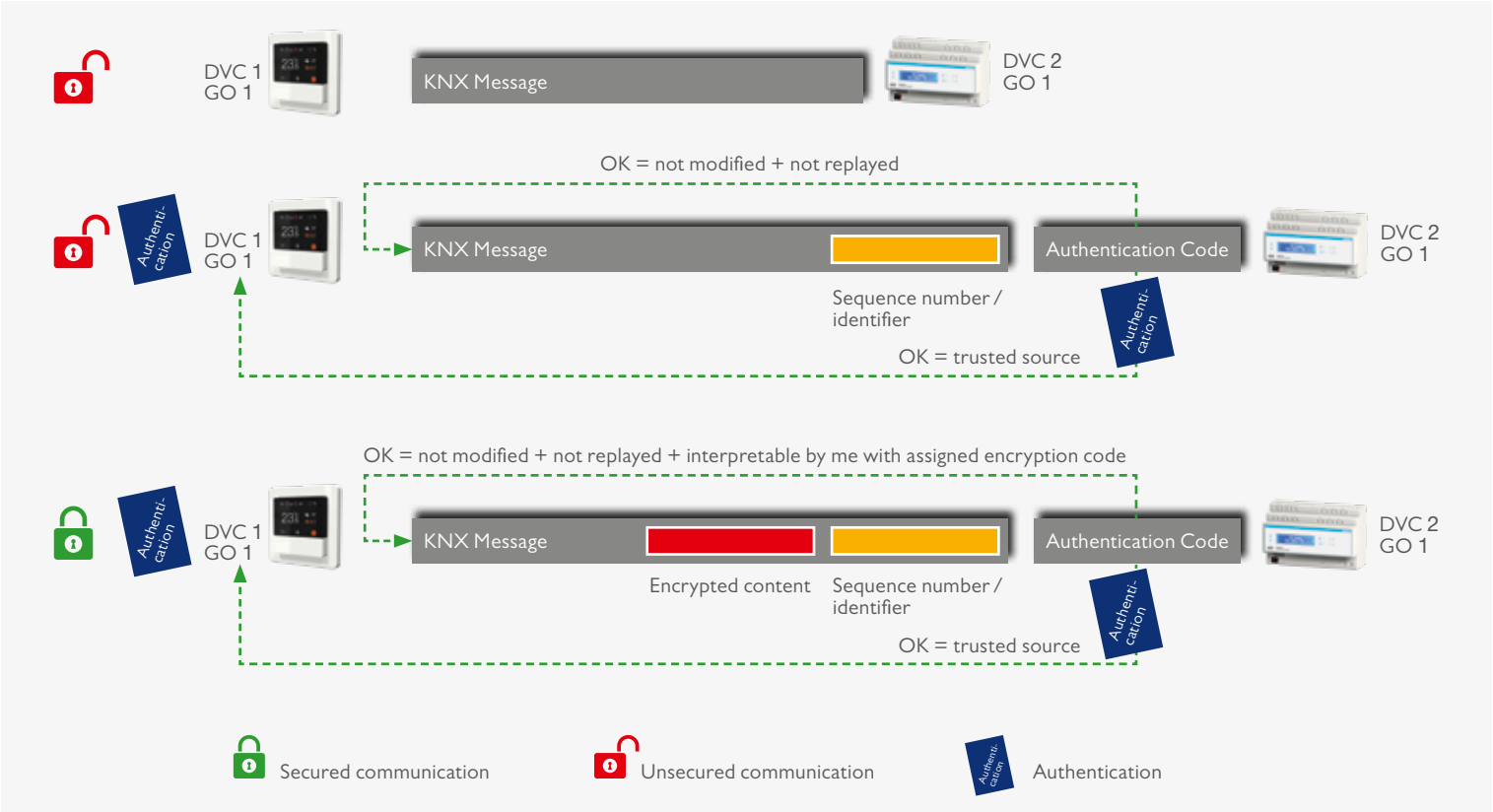
- De KNX Data Secure en KNX IP Secure mechanismen zorgen ervoor dat apparaten een beveiligd communicatiekanaal tot stand kunnen brengen en garanderen zo:
- de integriteit van de gegevens, d.w.z. voorkomen dat een aanvaller controle krijgt door gemanipuleerde frames te injecteren. KNX maakt dit mogelijk door aan elk bericht een authenticatiecode toe te voegen: deze toegevoegde code maakt het mogelijk om te verifiëren of het bericht niet is gewijzigd en of het daadwerkelijk afkomstig is van de vertrouwde communicatiepartner.
- de actualiteit van de gegevens, d.w.z. voorkomen dat een aanvaller frames opneemt en deze op een later tijdstip afspeelt zonder de inhoud te manipuleren. KNX Data Secure maakt dit mogelijk via een sequentienummer en KNX IP Secure via een sequentie-identifier.
- de vertrouwelijkheid van de gegevens, d.w.z. versleuteling van het netwerkverkeer zodat een aanvaller zo weinig mogelijk inzicht in de werkelijk verzonden gegevens heeft. Bij de versleuteling van KNX-netwerkverkeer garanderen KNX-apparaten minstens een versleuteling volgens de AES-128 CCM-algoritmen in combinatie met een symmetrische sleutel.

Een symmetrische sleutel betekent dat dezelfde sleutel wordt gebruikt door zowel de verzender om een uitgaand bericht te beveiligen (authenticatie + vertrouwelijkheid!) als door de ontvanger(s) om dit bericht te verifiëren bij ontvangst.
KNX Data Secure apparaten gebruiken een langer KNX-telegramformaat bij het verzenden van geauthenticeerde en gecodeerde gegevens. Dit heeft geen effect op de reactiesnelheid van apparaten. Bij KNX Data Secure worden de apparaten op de volgende manier beschermd:

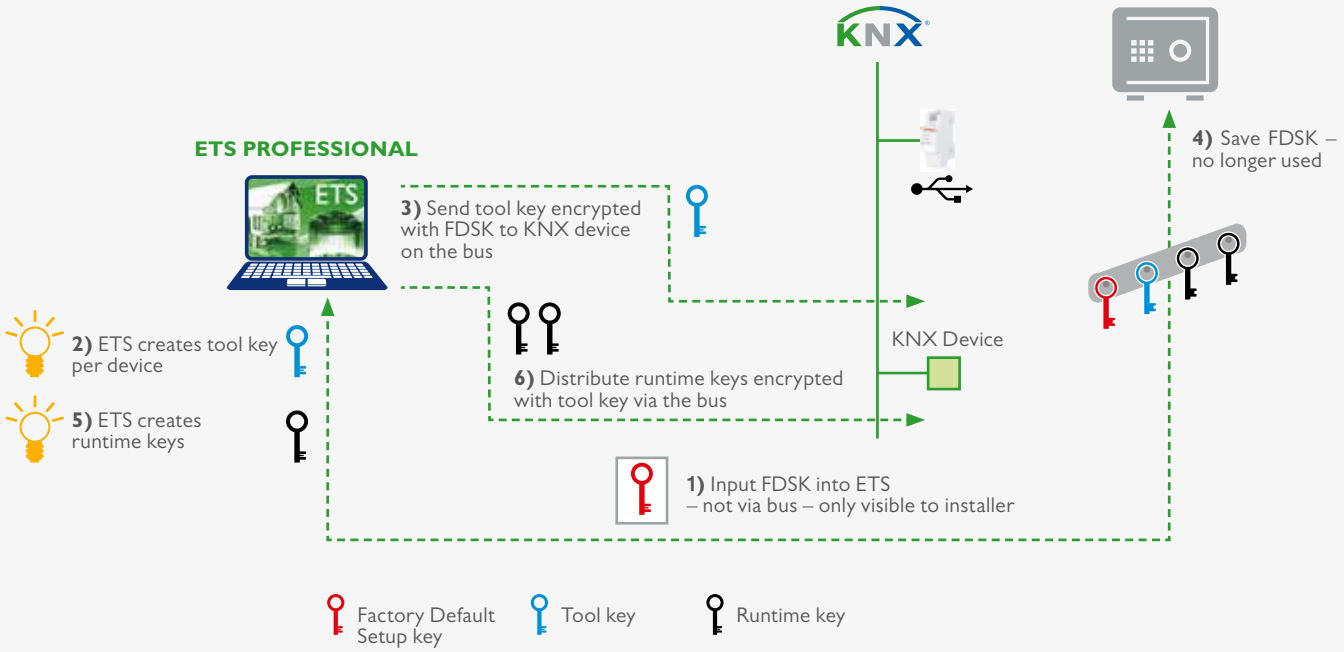
- Een apparaat wordt met een unieke FDSK (Factory Device Set up Key) geleverd.
- De installateur voert deze FDSK in de ETS-configuratietool in (deze actie wordt in ieder geval niet via de bus uitgevoerd).
- De configuratietool maakt een apparaatspecifieke gereedschapssleutel aan.
- ETS verstuurt de gereedschapssleutel via de bus naar het apparaat dat moet worden geconfigureerd. Dit bericht wordt echter versleuteld en geauthenticeerd met de eerder ingevoerde FDSK. Noch het gereedschap, noch de FDSK-sleutel worden op enig moment als platte tekst via de bus verzonden.
- Het apparaat aanvaardt vanaf dan enkel nog de gereedschapssleutel voor de verdere configuratie met de ETS. De FDSK wordt tijdens de daaropvolgende communicatie niet meer gebruikt, tenzij de fabrieksinstellingen van het apparaat worden gereset. Hierna worden alle beveiligde gegevens in het apparaat gewist.
- ETS maakt runtime sleutels (zoveel als nodig) aan voor de groepscommunicatie die moet worden beveiligd.
- ETS verstuurt deze runtime sleutels via de bus naar het apparaat dat moet worden geconfigureerd. Dit bericht wordt echter versleuteld en geauthenticeerd met de gereedschapssleutel. De runtime sleutels worden op geen enkel moment als platte tekst via de bus verzonden.

Bij KNX IP Secure wordt er op de volgende manier een beveiligde verbinding (tunnelling of apparaatbeheer) tot stand gebracht:

- Zowel de client als de server maken een individueel openbaar/privésleutelpaar aan. Dit wordt een asymmetrische versleuteling genoemd.



Overzicht van de KNX Data Secure mechanismen

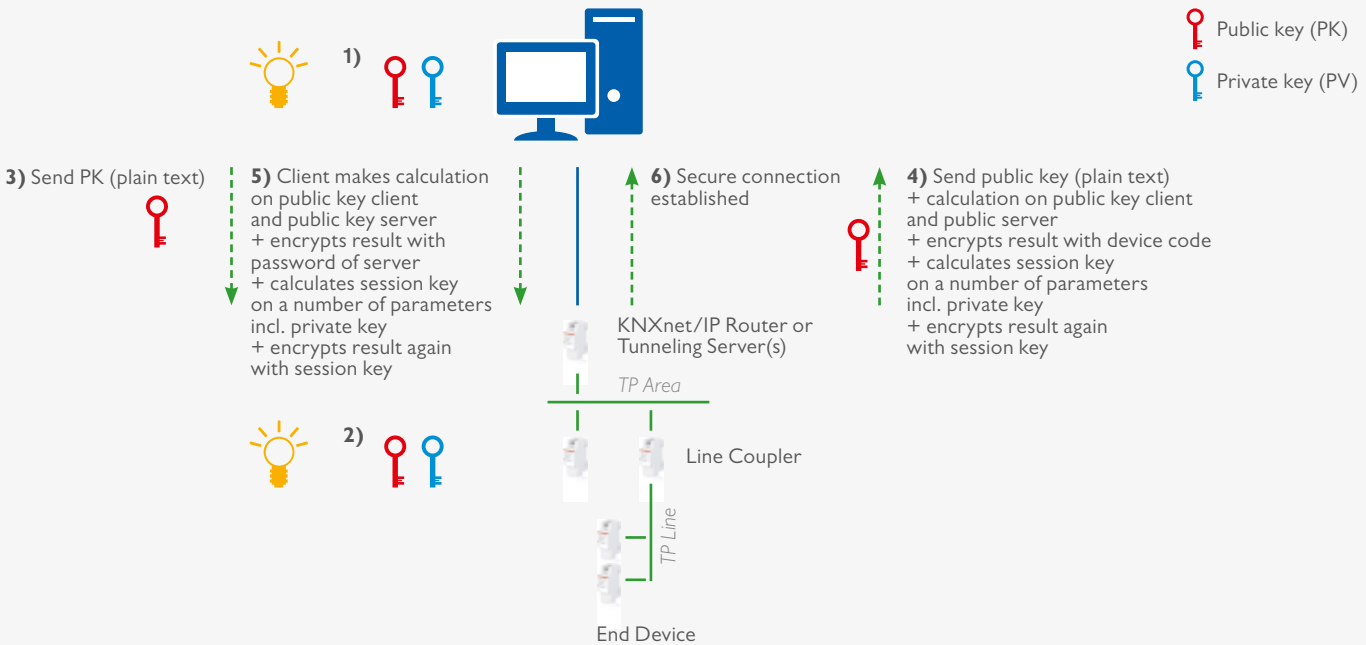


Procedure voor de beveiliging van KNX-apparaten

- De client verstuurt zijn openbare sleutel als platte tekst naar de server.
- De server antwoordt met zijn openbare sleutel in platte tekst, aangevuld met het resultaat van de volgende berekening: de server berekent de XOR-waarde van zijn openbare code met de openbare sleutel van de client, versleutelt deze met de apparaatcode om zich bij de client te authenticeren en versleutelt deze een tweede maal met de berekende sessiesleutel.
- De authenticatiecode van het apparaat wordt ofwel door ETS tijdens de configuratie of door de gereedschapssleutel toegekend. Deze authenticatiecode van het apparaat moet worden verstrekt aan de operator van de visualisatie die een beveiligde verbinding met de betrokken server tot stand wil brengen.
- De client voert dezelfde XOR-bewerking uit, maar machtigt zichzelf door deze eerst met een van de wachtwoorden van de server en nog een tweede keer met de sessiesleutel te versleutelen. We wijzen erop dat het gebruikte versleutelingsalgoritme (Diffie Hellmann) ervoor zorgt dat de sessiesleutel van de client en de server identiek zijn. De wachtwoorden van de server moeten worden verstrekt aan de operator van de visualisatie die een beveiligde verbinding met de betrokken server tot stand wil brengen.

We merken het volgende op met betrekking tot de hierboven beschreven maatregelen om de runtime communicatie te beschermen:

- KNX Data Secure apparaten kunnen zonder probleem naast 'klassieke' KNX-apparaten worden gebruikt. Dit betekent dat KNX data en IP Secure als bijkomende veiligheidsmaatregel kunnen worden geïmplementeerd.
- Als een installateur verkiest om een KNX IP Secure apparaat



Een KNX IP Secure verbinding tot stand brengen

in een IP backbone te gebruiken, moeten alle IP-koppelaars en alle KNX IP-apparaten in deze backbone van het type KNX IP Secure zijn.
- Als een installateur - op vraag van een klant - voor een functie een KNX Secure apparaat heeft gebruikt om de runtime communicatie te beveiligen, moet elke communicatiepartner van dit apparaat ook KNX Secure ondersteunen voor de gekoppelde functie. Met andere woorden, een communicatieobject van een KNX Secure apparaat kan niet eenmaal aan een beveiligd groepsadres en eenmaal aan een gewoon groepsadres worden gekoppeld.

Apparaten die KNX Data en IP Secure ondersteunen, kunnen door de 'X' op het productetiket van 'klassieke' KNX-toestellen worden onderscheiden.
KNX IP Secure en KNX Data Secure worden vanaf ETS 5.5 ondersteund. ETS maakt het mogelijk om nieuwe KNX Secure apparaten te configureren en ook om defecte KNX Secure apparaten te vervangen.

KNX AAN BEVEILIGINGSSYSTEMEN KOPPELEN

De koppeling van KNX aan toepassingen zoals inbraak-/brandbeveiligings-/deuropenings- systemen wordt uitgevoerd via:
- KNX apparaten of interfaces met passende certificatie door lokale verliesverzekeraars;
- potentiaalvrije contacten (binaire ingangen, drukknopinterfaces ...);
- geschikte interfaces (RS232 ...) of gateways: in dit geval moet ervoor worden gezorgd dat de KNX-communicatie geen veiligheidsrelevante functies in het veiligheidsgedeelte van de installatie kan activeren.

ONGEOORLOOFDE BUSTOEGANG OPSPOREN

Uiteraard kan de bus worden gemonitord en kan ongebruikelijk verkeer worden opgespoord.
KNX Secure apparaten houden de hacks bij in de logbestanden van beveiligingsfouten. Op deze manier is het op elk moment mogelijk om na te gaan of de KNX-installatie aan beveiligingsaanvallen werd blootgesteld.
Sommige apparaattypes kunnen detecteren of een ander apparaat telegrammen met hun individuele adres verstuurt. Dit wordt niet spontaan in het netwerk aangekondigd, maar kan in PID_DEVICE_CONTROL worden gelezen.
Zeer recente implementaties kunnen de PID_DOWNLOAD_COUNTER al vertonen.
Door de uitgelezen waarde (periodiek) met een referentiewaarde te vergelijken, worden wijzigingen in de configuratie van het apparaat gesignaleerd.

NALEVING VAN DE EUROPESE AVG-VERORDENING

AVG is een afkorting van Algemene Verordening Gegevensbescherming (zie https://ec.europa.eu/info/law/law-topic/data-protection_nl).
Deze verordening heeft als doel om de wetgeving inzake gegevensbescherming in heel Europa te harmoniseren.
Om aan de AVG-verordening te voldoen, overhandigt de elektricien het ETS-projectbestand aan de klant. Vervolgens ondertekenen de elektricien en de klant een verklaring inzake gegevensbescherming.
Gegevens die KNX-apparaten genereren, mogen enkel worden gebruikt voor afstandsbediening van het apparaat door de klant (via App), voor diagnosedoeleinden en voor verdere producttontwikkeling. Ze mogen niet voor gepersonaliseerde publiciteit worden gebruikt.

Literatuur

[1] AN 158 KNX Data Security
[2] AN 159 KNX IP Secure
[3] Volume 3/8/x KNXnet/IP Specifications

Smart home and building solutions.
Global. Secure. Connected.